Requirements for this paper:

Multiple choice cards: ☐	Non-programmable calculator: ☐		Open book examination ☐
Graph paper: ☐	Laptop: ☐		

EKSAMEN/ EXAMINATION:	Exam June 2017/Eksamen Junie 2017	KWALIFIKASIE RIGTING/ / QUALIFICATION :	**BSc IT Hons**

MODULEKODE/ MODULE CODE:	**ITRI615**	DUUR/ DURATION:	2 ½ hours 2 ½ ure
MODULE BESKRYWING/ SUBJECT:	Computer Security I Rekenaar Sekuriteit I	MAKS / MAX:	80

EKSAMINATOR(E)/ EXAMINER(S):	Dr C van der Vyver	DATUM / DATE:	**26/6/2017**
		TYD / TIME:	**9:00**
MODERATOR:	Dr M Kirlidog		

1. Discuss threats to a computing system by also referring to the four main types of threats.
   Bespreek bedreigings aan rekenaarstelsels deur ook te verwys na die vier hoof tipes bedreigings. **(8)**

2. What are some of the aspects that can enhance the effectiveness of security controls?
   Wat is sommige van die aspekte wat die effektiwiteit van sekuriteitsmaatstawwe kan verbeter? **(4)**

3. In the beginning of encryption several characteristics were proposed that define a good cipher. What are these characteristics?
   In die begin van enkripsie is verskeie eienskappe voorgestel wat 'n goeie cipher definiëer. Wat is hierdie eienskappe? **(5)**

4. Describe the working and the purpose of hash functions.
   Beskryf die werking en die doel van hash funksies. **(4)**

5. Briefly discuss the concept of malicious programs.
   Bespreek die konsep van kwaadwillige programme kortliks. **(3)**

6. What are the three main principles of software engineering that assist with the prevention of program threats? Discuss each principle briefly.
   Wat is die drie hoof beginsels van sagteware-ingenieurswese wat help met die voorkoming van programbedreigings? Bespreek elke beginsel kortliks. **(6)**

7. Separation is the basis of protection in operating systems. What are some of the ways in which this separation can be achieved?
   Skeiding is die basis van beskerming in bedryfstelsels. Wat is sommige van die maniere hoe hierdie skeiding bereik kan word? **(4)**

8. Name some of the many protection mechanisms that exist for memory and address protection.
   Noem sommige van die vele beskermingsmeganismes wat bestaan vir geheue en adres beskerming. **(6)**

9. Discuss the mechanisms that were introduced for file protection.
   Bespreek die meganismes wat bekendgestel is vir lêer beskerming. **(8)**

10. When can we refer to software as trusted software? What are the characteristics we typically look for?
    Wanneer kan ons verwys na sagteware as vertroude sagteware? Wat is die eienskappe wat ons tipies voor soek? **(6)**

11. There are several important design principles essential for security and for building a trusted operating system. What are these principles?
Daar is verskeie belangrike ontwerpsbeginsels wat krities is vir sekuriteit en vir die bou van 'n vertroude bedryfstelsel. Wat is hierdie beginsels? (8)

12. Name and briefly discuss the three techniques that are available to seek out vulnerabilities and eliminate their effects in trusted operating systems.
Noem en bespreek die drie tegnieke wat beskikbaar is om kwesbaarhede uit te soek in vertroude bedryfstelsels en hulle effekte te elimineer kortliks. (6)

13. Discuss fire suppression by referring to automatic detection systems, manual and automatic apparatus and also discussing gaseous suppression systems.
Bespreek brandbestryding deur te verwys na outomatiese opsporingstelsels, hand- en outomatiese apparaat en ook gas gebaseerde onderdrukkingstelsels te bespreek. (12)

TOTAL/TOTAAL: 80